Industrial Cybersecurity

In 2022, manufacturing became the most targeted industry for cyber attacks, a product of the combination of legacy systems, outdated software, and a low tolerance for downtime. Ensuring the security of a shop floor prior to a rollout of smart IoT systems is a necessary first step in creating a smart factory. Through the process of assessing and prioritizing risks, there a number of tools that can be used to mitigate those risks and create a more resilient and secure network architecture.

Why is Cybersecurity critical?

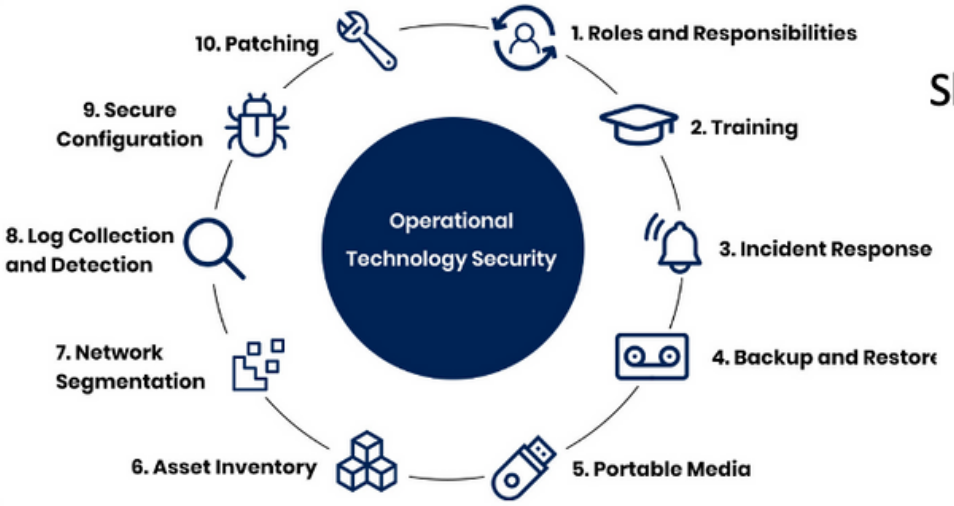
- Required for OT deployment
- Manufacturing targeted
- Downtime prevention
- Legacy systems still in use

How is it accomplished?

- Assess vulnerabilities & risks
- Protected network architecture
- Response and resilience plan
- Data encryption & protection

Recommendations

- Keep all software updated
- Manage IT-OT convergence
- Regular training & testing
- Access controls based on roles



Shop Floor Impacts

- Business continuity
- Regulatory compliance
- Protect customer IP
- Prevent downtime

Additional Suppliers for Industrial Cybersecurity

Fortinet offers a number of solutions to help create a "security fabric" for operational technology (OT) networks. This includes switches, firewalls, and other solutions to monitor and alert users about threats and risks, creating a secure and responsive architecture.

Finite State provides a platform to generate and manage a software bill of materials (SBOM) for all software and firmware residing in the supply chain. This SBOM is used to inform the asset user or OEM of vulnerabilities, risk levels, and available updates to eliminate or mitigate the risks.

Phoenix Contact's industrial router provide safety and security at a machine level with advanced firewalls and secure VPN connectivity. This provides superior protection while also allowing for secure remote maintenance capabilities, making them a valuable component of machines connecting to OT networks.